EXHIBIT A

SUMMONS

IN THE SUPERIOR/STATE COURT OF GLYNN **COUNTY**

STATE OF GEORGIA

Dale Timms, individually and on behalf of all others similarly situated,

PLAINTIFF

VS.

Ascension St. Vincent's Coastal Cardiology, f/d/b/a Coastal Cardiology P.C.,

DEFENDANT

CIVIL ACTION NUMBER CE22-01200

SUMMONS

TO THE ABOVE NAMED DEFENDANT: **Ascension St. Vincent's Coastal Cardiology, f/d/b/a Coastal Cardiology P.C.**

You are hereby summoned and required to file with the Clerk of said court and serve upon the Plaintiff's attorney, whose name and address is:

Allison E. McCarthy
Law Offices of Allie McCarthy
1055 Prince Avenue, Suite 2
Athens, GA 30606

an answer to the complaint which is herewith served upon you, within 30 days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.

This 9th day of December, 19 2022.

Clerk of Superior/State Court

/s/Victoria A. Moore
BY

Deputy Clerk

INSTRUCTIONS: Attach addendum sheet for additional parties if needed, make notation on this sheet if addendum sheet is used.

FILED - MB
GLYNN CO. CLERK'S OFFICE
Filed 11/18/2022 5:55 PM
Accepted 11/21/2022 8:17 AM
CASE # CE22-01200
Ronald M Adams
CLERK SUPERIOR COURT

General Civil and Domestic Relations Case Filing Information Form

■ Superior or ☐ State Court of Glynn County

For Clerk Use Only

Date Filed 11/18/2022 (MM-DD-YYYY)

Case Number CE22-01200

Plaintiff(s)

Last	First	Middle I.	Suffix	Prefix
Timms,	Dale			

Defendant(s) Ascension St. Vincent's Coastal Cardiology, f/d/b/a Coastal Cardiology P.C.

Last	First	Middle I.	Suffix	Prefix

Plaintiff's Attorney Allison E. McCarthy **State Bar Number** 482220 **Self-Represented** ☐

Check one case type and one sub-type in the same box (if a sub-type applies):

General Civil Cases

- ☐ Automobile Tort
- ☐ Civil Appeal
- ☐ Contempt/Modification/Other Post-Judgment
- ■ Contract
- ☐ Garnishment
- ☐ General Tort
- ☐ Habeas Corpus
- ☐ Injunction/Mandamus/Other Writ
- ☐ Landlord/Tenant
- ☐ Medical Malpractice Tort
- ☐ Product Liability Tort
- ☐ Real Property
- ☐ Restraining Petition
- ☐ Other General Civil

Domestic Relations Cases

- ☐ Adoption
- ☐ Contempt
  - ☐ Non-payment of child support, medical support, or alimony
- ☐ Dissolution/Divorce/Separate Maintenance/Alimony
- ☐ Family Violence Petition
- ☐ Modification
  - ☐ Custody/Parenting Time/Visitation
- ☐ Paternity/Legitimation
- ☐ Support – IV-D
- ☐ Support – Private (non-IV-D)
- ☐ Other Domestic Relations

☐ Check if the action is related to another action pending or previously pending in this court involving some or all of the same: parties, subject matter, or factual issues. If so, provide a case number for each.

Case Number _____ Case Number _____

■ I hereby certify that the documents in this filing, including attachments and exhibits, satisfy the requirements for redaction of personal or confidential information in OCGA § 9-11-7.1.

☐ Is a foreign language or sign-language interpreter needed in this case? If so, provide the language(s) required.

Language(s) Required _____

☐ Do you or your client need any disability accommodations? If so, please describe the accommodation request.

IN THE SUPERIOR COURT OF GLYNN COUNTY
STATE OF GEORGIA

Dale Timms, individually and on behalf of all others similarly situated,

Plaintiff(s),

v.

Ascension St. Vincent's Coastal Cardiology, f/d/b/a Coastal Cardiology P.C.,

Defendant.

CASE NO.: CE22-01200
JUDGE HARRISON

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

1. Plaintiff(s) Dale Timms ("Plaintiff(s)"), individually and on behalf of all others similarly situated, bring this action against Defendant Ascension St. Vincent's Coastal Cardiology, formerly doing business as Coastal Cardiology, P.C. ("Coastal Cardiology" or "Defendant"), to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. This class action arises out of the recent data security incident (the "Data Breach") that was perpetrated against Defendant Coastal Cardiology, which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiff(s) and other past and current patients of Defendant Coastal Cardiology, the putative Class Members ("Class"). According to its notice letters, Coastal Cardiology became aware of this Data Breach on or about August 15, 2022.

3. The Private Information compromised in the Data Breach included certain personal or protected health information of current and former patients, including Plaintiff(s). This Private Information included, but is not limited to: the patient's name, address, email address, phone number, and insurance information, Social Security number, clinical information, billing, and insurance information.

4. The Private Information was compromised in what Coastal Cardiology refers to as a "security event" in which an "unauthorized party accessed systems within the legacy Coastal Cardiology network."[1] In other words, cybercriminals intentionally targeted Coastal Cardiology for the Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated patients' highly sensitive PII and PHI, including Social Security numbers. As a

[1] *See* Plaintiff Timms' Notice Letter, attached as Exhibit A.

result, the Private Information of Plaintiff(s) and Class remains in the hands of and under the control of those cyber-criminals.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for treatment.

6. Plaintiff(s) bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized access of an unknown third party and including in that notice precisely what specific types of information were accessed and taken by cybercriminals.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Coastal Cardiology's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendant disregarded the rights of Plaintiff(s) and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff(s)' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

9. In addition, Defendant Coastal Cardiology failed to properly monitor the computer network and systems that housed the Private Information. Had Coastal Cardiology properly monitored its computers, it would have discovered the intrusion sooner rather than allowing cybercriminals unimpeded access to the PII and PHI of Plaintiff(s) Class Members such that the system could be encrypted and exfiltrated.

10. Plaintiff(s) and Class Members now face a substantial and imminent risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant Coastal Cardiology collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names,

using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff(s) and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Accordingly, Plaintiff(s) brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) unjust enrichment; (vi) declaratory judgment; and (vii) breach of confidence.

16. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant.

PARTIES

17. Plaintiff Dale Timms is and at all times mentioned herein was an individual citizen of the State of Georgia, residing in the city of Brunswick (Glynn County), and is a patient of Coastal Cardiology. Mr. Timms received notice of the Data Breach dated October 13, 2022, attached in Exhibit A.

18. Defendant Ascension St. Vincent's Coastal Cardiology has its principal place of business located at 3226-A Hampton Avenue, Brunswick (Glynn County), Georgia, 31520.

19. Prior to either being merged with or acquired by Ascension St. Vincent in or about October 1, 2021, Coastal Cardiology, P.C. also had its principal place of business located at 3226-A Hampton Avenue, Brunswick (Glynn County), Georgia, 31520. Upon information and belief, Defendant Ascension St. Vincent's Coastal Cardiology acquired and took responsibility for both the assets and liabilities of the predecessor entity, Coastal Cardiology, P.C.

JURISDICTION AND VENUE

20. This Court has original jurisdiction over Defendant Coastal Cardiology, as it is a domestic profit corporation in good standing, organized under the laws of the State of Georgia, with its principal place of business in Brunswick (Glynn County), Georgia and a majority (if not all) of its business in the State of Georgia, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

21. This Court has personal jurisdiction over Defendant Coastal Cardiology, as the company has sufficient minimum contacts with the State of Georgia. Defendant Coastal Cardiology intentionally avails itself of the markets within this district to render the exercise of jurisdiction by this court just and proper. Defendant Coastal Cardiology does business in the State of Georgia (through, among other things, its health care services with class members) and the business being done in Georgia directly relates to the subject of this lawsuit, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

22. Venue is proper in because a substantial part of the events and omissions giving rise to these claims occurred in Brunswick, Glynn County, Georgia.

23. Upon information and belief, a federal district court would be forced to decline to exercise CAFA jurisdiction over this matter, if filed in the federal courts.

Pursuant to 28 U.S.C. § 1332(d)(4)(B), and based upon Coastal Cardiology's headquarters, its overwhelming presence and extensive business holdings in the State of Georgia, Plaintiff believes that "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State of Georgia."

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant Coastal Cardiology provides heart health services to patients in the State of Georgia. Defendant helps "prevent heart attack or stroke, and [it] help[s] [patients] manage high blood pressure, high cholesterol and irregular heartbeats."[2] The doctors specialize in heart and vascular health, vascular surgery, AFib and heart rhythm disorders, and heart surgery.[3]

25. Upon information and belief Coastal Cardiology was acquired by or merged with Ascension St. Vincent ("Ascension"), a non-profit and faith-based healthcare organization on or about October 1, 2021.[4] Through its network, Ascension operates more than 2,600 sites with over 150,000 associates and 40,000

---

[2] https://healthcare.ascension.org/locations/georgia/fljac/brunswick-ascension-st-vincents-coastal-cardiology

[3] *Id.*

[4] https://www.ascension.org/About?_ga=2.80874455.1163524403.1667924982-1810126549.1667924982

healthcare providers.[5] Its facilities are spread throughout 19 states and the District of Columbia.[6]

26. In the ordinary course of receiving medical care services from Defendant Coastal Cardiology, each patient and employee must provide (and Plaintiff(s) did provide) Defendant Coastal Cardiology with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information such as age and gender;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage;
- Banking and/or credit card information;

---

[5] *Id.*
[6] *Id.*

- Information pertaining to patients' health; and
- Information relation to employment or affiliation with Defendant.[7]

27. Defendant also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses.

28. Defendant Coastal Cardiology agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff(s) and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

29. Upon information and belief, Coastal Cardiology's HIPAA Privacy Policy is provided to every patient both prior to receiving treatment and upon request.

30. In its "Patient Rights and Responsibilities Notice," Coastal Cardiology tells its patients (including Plaintiff(s) and the Class) that they have the following rights, among others: "To expect your medical records will be kept confidential and released only with your written consent, in cases of medical emergency, or in response to court orders."[8]

---

[7] *E.g.*, https://ascension.org/PrivacyPolicy?_ga=2.147975159.1163524403.1667924982-1810126549.1667924982 (last accessed Nov. 9, 2022).
[8] *Id.*

31. Yet, through its failure to properly secure the Private Information of Plaintiff(s) and Class, Coastal Cardiology has not adhered to its own promises of patient rights.

32. The patient (and upon information and belief, employee) information held by Defendant Coastal Cardiology in its computer system and network included the highly sensitive Private Information of Plaintiff(s) and Class Members.

The Data Breach

33. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Coastal Cardiology.

34. According to the undated "Coastal Cardiology Notice" that Coastal Cardiology posted on its website, "[o]n August 15, 2022, we were alerted to a security event . . . " Its "investigation determined that an unauthorized party accessed systems within the legacy Coastal Cardiology network." [9]

35. According to its notice letters, "[t]he primary purpose of the legacy network was to retain data, including patient information, to meet regulatory requirements but it was not used for current business operations." [10]

---

[9] *Coastal Cardiology Notice*, Ascension, https://healthcare.ascension.org/public-notices (last accessed Nov. 9, 2022).
[10] *Id.*

36. Coastal Cardiology admits "the legacy record would have contained individuals' demographic and health information related to visits at Coastal Cardiology prior to October 5, 2021, including: name, address, email address, phone number, and insurance information, as well as Social Security number (if provided), clinical information, and billing and insurance information."[11]

37. According to its letters, "[n]o Ascension networks or systems, including the practice's current electronic medical record, were affected by this incident[,]" which suggests that this Data Breach only affected who were patients of the Georgia medical practice prior to October 5, 2021.[12] The notice letters do not indicate the oldest records that were encrypted and do not divulge the retention practices of Coastal Cardiology prior to the merger or acquisition.

38. Furthermore, "because the information was encrypted [Coastal Cardiology is] unable to access it" and Coastal Cardiology remains unable to determine what information was affected and cannot tell Plaintiff(s) and Class exactly what information was encrypted and exfiltrated.[13]

39. However, without further explanation, in its notice letter Coastal Cardiology claims that it takes the "protection and safeguarding of our patient

---

[11] *Id.*
[12] *Id.*
[13] *Id.*

information seriously"[14] Then it claims to be taking "steps to ensure a similar incident does not happen again." [15]

40. In other words, it appears that although Coastal Cardiology claims it takes the "protection and safeguarding of our patient information seriously" it did not even figure out that cybercriminals had been accessing the Private Information held on Coastal Cardiology's systems for almost 2 months, before notifying victims of the breach.[16]

41. The website Notice of Security Incident also states that some of the accessed "files contained patient information, including names, Social Security numbers, and clinical information."[17]

42. As reported to Department of Health and Human Services Office for Civil Rights ("DHH Report") on October 14, 2022, Coastal Cardiology's investigation revealed that the Private Information (including both PII and PHI) of 71,227 individuals was accessed in this Data Breach.[18]

43. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiff(s) and Class

---

[14] *See* Exhibit A
[15] *Id.*
[16] *See* Notice Letter, Ex. A
[17] *Coastal Cardiology Notice*, *supra* note 9.
[18] *Cases Currently Under Investigation*, U.S. Dep't of Health & Human Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 3, 2022).

Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff(s) and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Furthermore, Ascension's website includes a HIPAA privacy policy for 11 states, their pharmacy entity, and nursing homes. However, they fail to include a HIPAA privacy policy specifically for Georgia where Coastal Cardiology is located.[19]

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

45. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Coastal Cardiology, are well-aware of the risk of being targeted by cybercriminals.

46. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

---

[19] *Notice of Privacy Practices*, Ascension (2022), https://healthcare.ascension.org/npp.

47. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[20]

48. Individuals, like Plaintiff(s) and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

49. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

---

[20] Erika Harrell, *Victims of Identity Theft, 2018*, U.S. Dep't of Just. (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Nov. 9, 2022).

50. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[21]

51. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020s total of 1,108 and the previous record of 1,506 set in 2017.[22]

52. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, security executives who were polled predict an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these

---

[21] *Identity Theft and Your Social Security Number*, SSA (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Nov. 9, 2022).

[22] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Nov. 9, 2022).

preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[23]

53. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

54. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[24] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[25]

---

[23] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Nov. 9, 2022).

[24] *How We Can Help You: Ransomware*, FBI https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Nov. 9, 2022).

[25] *Id.*

55. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII and PHI both private and secure, Coastal Cardiology failed to take appropriate steps to protect the Private Information of Plaintiff(s) and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

56. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

57. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[26]

[26] *Editorial: Why Do Criminals Target Medical Records*, HIPAA J.(Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed Nov. 9, 2022).

58. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[27]

59. The HIPAA Journal article goes on to explain that patient records, like those stolen from Coastal Cardiology, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[28]

60. Data breaches such as the one experienced by Defendant Coastal Cardiology have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

---

[27] *Id.*
[28] *Id.*

61. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[29]

62. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[30]

63. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant Coastal Cardiology.

Defendant Fails to Comply with FTC Guidelines.

64. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

65. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for

---

[29] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited on Nov. 9, 2022).

[30] *5 Important Elements to Establish Data Security in Healthcare*, AdventHealth Univ. (May 21, 2020), https://www.ahu.edu/blog/data-security-in-healthcare (last visited Nov. 9, 2022).

businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[31] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[32]

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses like Coastal Cardiology's for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against

---

[31] *Protecting Personal Information: A Guide for Business*, FTC (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 9, 2022).
[32] *Id.*

unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In re LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

69. Defendant failed to properly implement basic data security practices.

70. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

72. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

73. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

74. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

75. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA.

77. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information (PHI).

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

79. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

80. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, " . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. § 164.40.

81. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant has Breached its Obligations to Plaintiff(s) and Class.

82. Defendant breached its obligations to Plaintiff(s) and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Coastal Cardiology's legacy computer systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

83. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing

ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff(s)' and Class Members' Private Information.

84. Accordingly, as outlined below, Plaintiff(s) and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft.

85. Data Breaches such as the one experiences by Coastal Cardiology's patients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

86. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[33] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B.

87. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff(s) and Class) must take after a breach like Coastal

---

[33] *See* U.S. Gov't Accountability Off., GAO-19-230, Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf (last accessed Nov. 10, 2022). *See* attached as Ex. B.

Cardiology's are both time consuming and of only limited and short-term effectiveness.[34]

88. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report"). [35]

89. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[36]

90. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

---

[34] *Id.*

[35] *See* U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown at 2, U.S. Gov't Acct. Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Nov. 3, 2022) ("2007 GAO Report").

[36] *See Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Nov. 9, 2022).

91. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

92. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[37]

93. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report at 29.

---

[37] *See, e.g.*, John T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

94. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

95. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff(s) and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff(s) and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

96. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[38]

97. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[39] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits,

---

[38] *A Cost Analysis of Healthcare Sector Data Breaches Health Sector Cybersecurity Coordination Center (HC3)* at 2, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf (citations omitted) (last accessed Nov. 9, 2022).

[39] *Identity Theft and Your Social Security Number*, *supra* note 21, at 1.

or apply for a job using a false identity.[40] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

98. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[41]

99. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable

---

[40] *Id.* at 4.

[41] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Nov. 9, 2022).

information and Social Security Numbers are worth more than 10x on the black market."[42]

100. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF(S)' EXPERIENCES

Plaintiff Dale Timms

101. Plaintiff Dale Timms is and at all times mentioned herein was an individual citizen residing in the State of Georgia, in the city of Brunswick (Glynn County).

102. Plaintiff Timms was a Coastal Cardiology patient prior to October 5, 2021, and since the merger with Ascension, is still a patient of Coastal Cardiology at all times relevant to this Complaint.

---

[42] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 9, 2022).

103. Plaintiff Timms received a Notice of Data Breach Letter, related to Coastal Cardiology's Data Breach that is dated October 13, 2022. *See* Exhibit A.

104. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files include "your demographic information such as your name, address, email address, phone number, and insurance information, as well as your Social Security number (if you provided), clinical information, and billing and insurance information." *See* Ex. A.

105. Plaintiff Timms is especially alarmed by the vagueness of her stolen extremely private medical information (PHI) and equally by the fact that her Social Security number was identified as among the breached data on Coastal Cardiology's computer system.

106. Since the Data Breach, Plaintiff Timms monitors her financial accounts for about 7 hours per week. This is more time than she spent prior to learning of Coastal Cardiology's Data Breach. Having to do this every week not only wastes her time as a result of Coastal Cardiology's negligence, but it also causes her great anxiety.

107. Starting after the Data Breach occurred, Plaintiff Timms began receiving an excessive number of spam calls and on the same cell phone number that she provided at Coastal Cardiology. These calls and emails are a distraction, must

be deleted, and waste her time each day. Once she received the Notice Letter, and given the timing of the Data Breach, she believes that the spam calls are related to her stolen PII.

108. In addition, Plaintiff Timms receives *many* spam emails and texts now, and which she did not typically receive before the Data Breach. She cannot figure out any explanation other than that these are related to Coastal Cardiology's Data Breach, which included her Private Information.

109. Since the breach occurred, she has been receiving mail addressed to her maiden name, which she never uses. Moreover, the spam phone calls she receives ask for her by her maiden name, which she never uses.

110. Plaintiff Timms is a disabled person, and this Breach has added to her stress, because she is worried that someone now has the ability to gain access to the few resources that she has, *e.g.*, Social Security benefits.

111. Plaintiff Timms has tried to mitigate the impact of the Data Breach by signing up for the free credit monitoring service offered by Defendant. However, she is aware that this service is offered for only a year, which is woefully inadequate.

112. Plaintiff Timms is aware that cybercriminals often sell Private Information, and that her Private Information could be abused months or even years after this Data Breach.

113. Had Plaintiff Timms been aware that Coastal Cardiology's computer systems were not secure, she would not have entrusted Coastal Cardiology with her PII and PHI.

PLAINTIFF(S)' AND CLASS MEMBERS' INJURIES

114. To date, Defendant Coastal Cardiology has done absolutely nothing to compensate Plaintiff(s) and Class Members for the damages they sustained in the Data Breach.

115. Defendant Coastal Cardiology has merely offered one year credit monitoring services through Experian IdentityWorks, a tacit admission that its failure to protect their Private Information has caused Plaintiff(s) and Class great injuries. *See* Ex. A. This one-year limitation is inadequate when victims are likely to face many years of identity theft.

116. Coastal Cardiology's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff(s)' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

117. Furthermore, Defendant Coastal Cardiology's credit monitoring offer and advice (*see* Ex. A) to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to investigate and

protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

118. Plaintiff(s) and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

119. Plaintiff(s)'and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

120. Plaintiff(s) and Class were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

121. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

122. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been forced to expend time dealing with the effects of the Data Breach.

123. Plaintiff(s) and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their

names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff(s) and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

124. Plaintiff(s) and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff(s) and Class Members.

125. Plaintiff(s) and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

126. Plaintiff(s) and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

127. Plaintiff(s) and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

128. Moreover, Plaintiff(s) and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of

Defendant on both its legacy systems and now on the Ascension networks, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

129. Further, as a result of Defendant's conduct, Plaintiff(s) and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

130. Defendant's delay in identifying and reporting the Data Breach caused additional harm. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft.

CLASS ACTION ALLEGATIONS

131. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other persons similarly situated.

132. Plaintiff(s) propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by Coastal Cardiology in or about August

2022 and for which it provided notice on or about October 2022 (the "Class").

133. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

134. Plaintiff(s) hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under the O.C.G.A. 9-11-23, *et seq.*

135. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff(s) at this time, but Coastal Cardiology has provided notice to HHS that the number of individuals whose files were breached is approximately 71,227 individuals.

136. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

137. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

138. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

139. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues.

Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

140. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

141. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

142. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

143. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiff(s) and Class Members)

144. Plaintiff(s) re-alleges and incorporates the above allegations as if fully set forth herein.

145. Defendant Coastal Cardiology required Plaintiff(s) and Class Members to submit non-public personal information in order to obtain healthcare/medical services.

146. By collecting and storing this data in Coastal Cardiology's computer network, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

147. Defendant owed a duty of care to Plaintiff(s) and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

148. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Coastal Cardiology and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

149. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

150. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

151. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also

because Defendant is bound by industry standards to protect confidential Private Information.

152. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

153. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

154. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

155. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

156. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff(s) and Class Members in an unsafe and unsecure manner.

157. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Second Count
Breach of Implied Contract
(On Behalf of Plaintiff(s) and Class Members)

158. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

159. When Plaintiff(s) and Class Members provided their Private Information to Defendant Coastal Cardiology in exchange for Defendant Coastal Cardiology's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

160. Defendant Coastal Cardiology solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff(s) and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

161. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

162. Plaintiff(s) and Class Members paid money to Defendant to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

163. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

164. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

165. Plaintiff(s) and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

166. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

167. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

168. Plaintiff(s) and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

169. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring

procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Third Count
Negligence *Per Se*
(On Behalf of Plaintiff(s) and All Class Members)

170. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

171. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

172. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff(s)' and Class Members' Private Information.

173. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

174. Defendant breached its duties to Plaintiff(s) and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable,

or adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

175. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

176. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff(s) and Class Members, Plaintiff(s) and Class Members would not have been injured.

177. The injury and harm suffered by Plaintiff(s) and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendant's breach would cause Plaintiff(s) and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

178. As a direct and proximate result of Defendant's negligent conduct, Plaintiff(s) and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Fourth Count
Breach of Fiduciary Duty
(On Behalf of Plaintiff(s) and Class Members)

179. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

180. In light of the special relationship between Defendant Coastal Cardiology and Plaintiff(s) and Class Members, whereby Defendant became guardian of Plaintiff(s)' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff(s) and Class Members, (1) for the safeguarding of Plaintiff(s)' and Class Members' Private Information; (2) to timely notify Plaintiff(s) and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

181. Defendant has a fiduciary duty to act for the benefit of Plaintiff(s) and Class Members upon matters within the scope of Coastal Cardiology's relationship with its patients and former patients, in particular, to keep secure their Private Information.

182. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

183. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff(s)' and Class Members' Private Information.

184. Defendant breached its fiduciary duties owed to Plaintiff(s) and Class Members by failing to timely notify and/or warn Plaintiff(s) and Class Members of the Data Breach.

185. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by otherwise failing to safeguard Plaintiff(s)' and Class Members' Private Information.

186. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of

Plaintiff(s) and Class Members; and (vii) the diminished value of Defendant's services they received.

187. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

Fifth Count
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiff(s) and All Class Members)

188. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

189. The State of Georgia recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

190. Plaintiff(s) and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

191. Defendant's conduct as alleged above intruded upon Plaintiff(s)' and Class Members' seclusion under common law.

192. By intentionally failing to keep Plaintiff(s)' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said

information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff(s)' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff(s)' and Class Members' private affairs in a manner that identifies Plaintiff(s) and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff(s) and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff(s) and Class Members.

193. Defendant knew that an ordinary person in Plaintiff(s)' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

194. Defendant invaded Plaintiff(s)' and Class Members' right to privacy and intruded into Plaintiff(s)' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

195. Defendant intentionally concealed from and delayed reporting to Plaintiff(s) and Class Members a security incident that misused and/or disclosed

their Private Information without their informed, voluntary, affirmative, and clear consent.

196. The conduct described above was at or directed at Plaintiff(s) and the Class Members.

197. As a proximate result of such intentional misuse and disclosures, Plaintiff(s)' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff(s)' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

198. In failing to protect Plaintiff(s)' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff(s)' and Class Members' rights to have such information kept confidential and private. Plaintiff(s), therefore, seek an award of damages on behalf of themselves and the Class.

Sixth Count
Unjust Enrichment
(On Behalf of Plaintiff(s) and Class Members)

199. Plaintiff(s) re-allege the above allegations as if fully set forth herein. Plaintiff(s) bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

200. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff(s) and the Class Members.

201. As such, a portion of the payments made by or on behalf of Plaintiff(s) and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

202. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff(s) and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

203. Defendant knew that Plaintiff(s) and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and

used the Private Information of Plaintiff(s) and Class Members for business purposes.

204. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s) and Class Members by utilizing cheaper, ineffective security measures. Plaintiff(s) and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

205. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff(s) and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

206. Defendant failed to secure Plaintiff(s)' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff(s) and Class Members provided.

207. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

208. If Plaintiff(s) and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

209. Plaintiff(s) and Class Members have no adequate remedy at law.

210. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private

Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

211. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

212. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff(s) and Class Members overpaid for Defendant's services.

Seventh Count
Declaratory Judgment
(On Behalf of Plaintiff(s) and Class Members)

213. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

214. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

215. An actual controversy has arisen in the wake of the Coastal Cardiology data breach regarding its present and prospective common law and other duties to

reasonably safeguard its patients' Private Information and whether Coastal Cardiology is currently maintaining data security measures adequate to protect Plaintiff(s) and Class members from further data breaches that compromise their Private Information.

216. Plaintiff(s) allege that Coastal Cardiology's data security measures remain inadequate. Plaintiff(s) will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

217. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Coastal Cardiology continues to owe a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Coastal Cardiology continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

218. The Court also should issue corresponding prospective injunctive relief requiring Coastal Cardiology to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

219. If an injunction is not issued, Plaintiff(s) and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Coastal Cardiology. The risk of another such breach is real, immediate, and substantial. If another breach at Coastal Cardiology occurs, Plaintiff(s) and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

220. The hardship to Plaintiff(s) and Class Members if an injunction does not issue exceeds the hardship to Coastal Cardiology if an injunction is issued. Among other things, if another massive data breach occurs at Coastal Cardiology, Plaintiff(s) and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Coastal Cardiology of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Coastal Cardiology has a pre-existing legal obligation to employ such measures.

221. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Coastal Cardiology, thus eliminating the additional injuries that would result to Plaintiff(s) and the patients' whose Private Information would be further compromised.

Eighth Count
Breach of Confidence
(On Behalf of Plaintiff(s) and All Class Members)

222. Plaintiff(s) reallege and incorporate by reference the allegations above as if fully set forth herein.

223. At all times during Plaintiff(s)' and Class Members' interaction with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff(s)' and Class Members' Private Information.

224. As alleged herein and above, Defendant's relationship with Plaintiff(s) and Class Members was governed by terms and expectations that Plaintiff(s)' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

225. Plaintiff(s) and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit Private Information to be disseminated to any unauthorized parties.

226. Plaintiff(s) and Class Members also provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect such highly sensitive information from unauthorized disclosure.

227. Defendant voluntarily received in confidence Plaintiff(s)' and Class Members' Private Information with the understanding that it would not be disclosed or disseminated to the public or any unauthorized third parties.

228. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff(s)' and Class Members' Private Information, Plaintiff(s)' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff(s)' and Class Members' confidence, and without their express permission.

229. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff(s) and Class Members have suffered damages.

230. But for Defendant's disclosure of Plaintiff(s)' and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff(s)' and Class Members' protected Private Information, as well as the resulting damages.

231. The injury and harm Plaintiff(s) and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff(s)' and Class Members' Private Information.

232. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching to prevent, detect, contest, and recover from financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of past and current customers in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

233. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff(s) and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff(s) and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff(s) and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff(s) demand a trial by jury on all claims so triable.

Dated: November 10, 2022

Respectfully submitted,

/s/ Allison E. McCarthy
Allison E. McCarthy
GA Bar No. 482220
LAW OFFICES OF ALLIE MCCARTHY
1055 Prince Avenue, Suite 2
Athens, GA 30606
Phone: (678) 637-6243
attorneymccarthy@gmail.com

Gary E. Mason*
Danielle Perry*
Lisa A. White*
MASON LLP
5101 Wisconsin Avenue NW, Suite 305

Washington, DC 20016
Telephone: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff
**pro hac vice to be filed*

EXHIBIT A

Ascension
St. Vincent's

[redacted]

October 13, 2022

DALE TIMMS
627 HALSEY ST
BRUNSWICK GA 31525-8804

Dear Dale Timms,

We are writing to tell you about an incident that affected some of your protected health information, or PHI. On August 15, 2022, we were alerted to a security event involving Ascension St. Vincent's Coastal Cardiology's legacy systems including the electronic medical record ("EMR"). Upon discovery, we immediately secured the legacy network, but unfortunately not before some of the information was encrypted by ransomware. We take the privacy and security of your information very seriously and we sincerely apologize for this incident. Please know that Ascension's networks and Coastal Cardiology's current (active) medical record system were not affected by this incident.

Upon discovery of this incident, we took immediate actions to investigate. We hired a third-party forensic team to assist us with investigating how the perpetrators gained access to encrypt the information. Additionally, we notified law enforcement about the event and will continue to cooperate with them. Our investigation has determined that an unauthorized third-party accessed systems within the legacy Coastal Cardiology network. The primary purpose of the legacy network was to retain data, including patient information, to meet regulatory requirements but it was not used for current business operations. At this time, based on our investigation, we do not believe that any information was removed from the systems affected by this event or that it has been misused or shared by the perpetrators.

Unfortunately, because the information was encrypted and we are unable to access it, we are unable to tell you exactly what information was affected. However, the legacy EMR would have contained all of your personal information and treatment records related to your visits at Coastal Cardiology prior to October 5, 2021. This includes your demographic information such as your name, address, email address, phone number, and insurance information, as well as your Social Security number (if you provided), clinical information, and billing and insurance information.

Although there is no indication that your information has been misused, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: December 29, 2022 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com
- Provide your activation code: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (855) 896-4449 by December 29, 2022. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian. Please find additional information about Experian Identity Works at the end of this letter. You can also review the enclosed information about additional ways to protect yourself from credit or identity theft and how to place holds on your accounts.

We take the protection and safeguarding of our patient information seriously and we have taken steps to ensure a similar incident does not happen again. Ascension initiated a security risk assessment, realigned staff responsibilities, removed access rights to the legacy system and retrained associates. We will also report this incident to the Office for Civil Rights in accordance with our obligations under the HIPAA Rules.

We sincerely apologize for any stress or inconvenience this incident may have caused. If you have any questions regarding this issue or you would like further information or assistance, please reach out to our dedicated call center team at (855) 532-1247, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. Holidays

Sincerely,

Peggy Panos

Peggy Panos
Compliance Senior Director

Additional Information

We are also providing the below information as ways you can monitor your information from fraud, including how to place fraud alerts and security freezes on your accounts/information.

Consumer Reporting Agencies

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. Once you receive your credit reports, verify the information is correct and review them for differences. Identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting company.

You may also purchase additional copies of your credit report or place a 90-day fraud alert on your credit file if you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. A fraud alert placed with one agency will be shared by that credit reporting agency with the other two agencies (i.e., you only need to request a fraud alert with one of the below agencies).

You can also place a security freeze on your credit report which will prevent lenders and others from accessing your credit report entirely, which also prevents them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is completed by contacting each of the credit reporting companies separately (i.e., you must request a security freeze from each of the below agencies).

Equifax: P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com

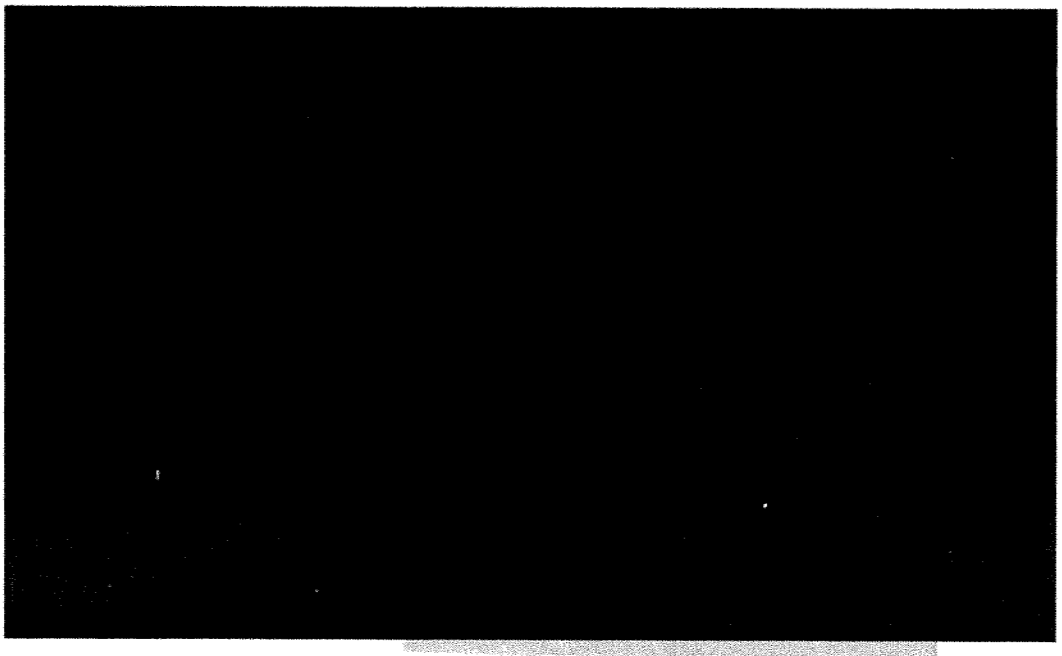
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 2000, Chester, PA 19016, 1-800-680-7289 (fraud alerts), 1-888-909-8872 (credit freeze), www.transunion.com

Federal Trade Commission

You can contact the FTC regarding fraud alerts or security concerns at:

- Address: Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580
- Phone: (202) 326-2222 or the Consumer Response Center toll free at 1-877-FTC-HELP (1-877-382-4357)
- Website: https://www.ftc.gov/contact



Additional Details Regarding Your 12 Month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 896-4449. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

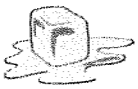
EXHIBIT B

Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.[1]

[1]GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C.: Mar. 30, 2017).

Figure 3: What Can Consumers Do After a Data Breach?

Prevent Fraud on New Credit Accounts		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Place a credit freeze** on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies.	• Prevents identity thieves from opening new credit accounts in an individual's name—where credit reports are required. • Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated.	• Consumers must request a freeze at each of the three agencies separately. • Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports. • Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card). • Freezes do not prevent other types of harm, such as tax refund or medical identity fraud. • Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks). • Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).
 **Place a fraud alert** at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed.	• Fraud alerts let businesses know that a consumer may have been a victim of fraud. • Businesses must take extra steps to verify the identity of the individual seeking to open accounts. • Members of the military can place active duty alerts.	• Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert. • Victims of identity theft can place extended fraud alerts that last for 7 years. • Fraud alerts still allow access to credit reports. • Businesses that do not use the three agencies will not see the alert.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Some Types of Fraud on Financial Accounts		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Review free credit reports every 12 months** (from Equifax, Experian, and TransUnion) at annualcreditreport.com.	• Can help consumers spot suspicious activity or fraud involving credit accounts.	• Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year.
 **Review bank and other financial account statements regularly or set up free automatic alerts.**	• Can alert consumers to suspicious activity on their accounts.	• The availability and features of alerts may vary among financial institutions.
 **Consider enrolling in credit or identity monitoring services.**	• Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card). • Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the "dark web").	• These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud. • Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts. • Identity monitoring also cannot prevent fraud. • It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts. • These services may be part of a package of identity theft services, including restoration services, or identity theft insurance. • Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer. • Paid services typically cost $5–$30 a month.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Other Types of Identity Theft or Fraud		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Mobile Phone or Utility Account Fraud**		
Review mobile phone and utility bills regularly.	• Can spot suspicious activity on existing accounts.	• Consumers with credit freezes may need to lift them before applying for new utility or phone accounts.
 **Medical Identity Theft**		
Review medical bills and health insurance explanations of benefits.	• Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive.	• Consumers who spot problems can contact fraud departments at health insurers.
 **Identity Theft Tax Refund Fraud**		
File tax returns early.	• Provides less time for a fraudster to file in an individual's name.	• Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS.
 **Government Benefits Fraud**		
Set up an online account at the Social Security Administration and check it regularly.	• Can spot suspicious activity, such as benefits redirected to another address.	• Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

How to Respond after Identity Theft		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
Visit identityTheft.gov to set up an account, fill out, and file necessary reports.	• Helps users determine what steps to take depending on the type of information stolen or type of identity theft. • Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities. • Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS. • Provides information on what companies to contact and how to remove incorrect information.	• The Federal Trade Commission (FTC) also has a telephone help line and online chat feature.
Contact state or local government resources, such as consumer protection help lines or victim services offices.	• Some states and local governments can provide one-on-one assistance.	• States and localities vary in the services offered.
Consider using commercial identity restoration services.	• Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf.	• Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information. • May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost $5–$30 a month and free services may only be offered for 1-2 years.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Protect Personal Information in Other Ways		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Adopt Good Practices for Online Accounts** • Protect passwords and do not re-use them. • Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account). • Choose strong passwords and consider using a software application that helps manage passwords. • Do not click on links in emails or open attachments from unknown senders. • Remember that public WiFi may not be secure.	• Can prevent unauthorized access to online accounts and other data intrusions.	• While personal security practices are important, consumers have limited control over how private entities secure their data.
 **Protect social media accounts** by checking privacy settings, and consider limiting information shared.	• Restricts how much information is visible to strangers and their ability to misuse it.	• Privacy terms and conditions can change, so it is important to check settings periodically.
 **Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).**	• Prevents identity thieves from obtaining information that can be used to commit fraud.	• Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information. • Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at ftc.gov/complaint.
 **Shred documents and mail with Social Security numbers or other personal information.**	• Prevents identity thieves from finding sensitive information in trash.	• Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected. • Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230